

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ
по лабораторной работе №7
по дисциплине «Сети и телекоммуникации»
Тема: Лабораторная работа 7. Сетевые экраны. IPTABLES

Студентка гр. 9382

Голубева В.П.

Преподаватель

Лавров А.А.

Санкт-Петербург

2021

Цель работы.

Целью работы является изучение принципов работы с сетевыми экранами.

Задание.

- 1) Заблокировать доступ по IP-адресу Ub1 к Ub3.2.
- 2) Заблокировать доступ по порту X на Ub1.
- 3) Заблокировать доступ к порту X на Ub3 от UbR. Проверить возможность доступа с Ub1.
- 4) Полностью запретить доступ к Ub3. Разрешить доступ к порту X.
- 5) С помощью правила по умолчанию обеспечить блокировку всех входящих и исходящих пакетов узла Ub3, исключая пакеты управления сетью (протокол ICMP). Убедиться, что Ub3 принимает и отвечает на запросы команды ping, но не отвечает на запросы протокола TCP.
- 6) Запретить подключение к Ub1 по порту X. Настроить логгирование попыток подключения по порту X.
- 7) Заблокировать доступ по порту X к Ub3 с Ub1 по его MAC-адресу.
- 8) Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов X.
- 9) Разрешить только одно ssh подключение к UbR. Значение X своё для каждого задания в каждом варианте.

Вариант 4.

2 X=24, 3 X= 74, 4 X=24, 6 X= 74, 7 X= 14, 8 X=14-74

Выполнение работы.

Были развёрнуты три виртуальные машины убунту — ub1, ub2, ub3.

ub1 [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
root@buntUs:/home/bla# ifconfig -a
enp0s3   Link encap:Ethernet  HWaddr 08:00:27:a7:07:1d
         inet addr:192.168.0.11  Bcast:192.168.0.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fea7:71d/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:83 errors:0 dropped:0 overruns:0 frame:0
         TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:18866 (18.8 KB)  TX bytes:4220 (4.2 KB)
```

ub2 [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
root@buntUs:/home/bla# ifconfig -a
enp0s3   Link encap:Ethernet  HWaddr 08:00:27:4a:2c:da
         inet addr:192.168.0.12  Bcast:192.168.0.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe4a:2cda/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:89 errors:0 dropped:0 overruns:0 frame:0
         TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:19700 (19.7 KB)  TX bytes:4220 (4.2 KB)
```

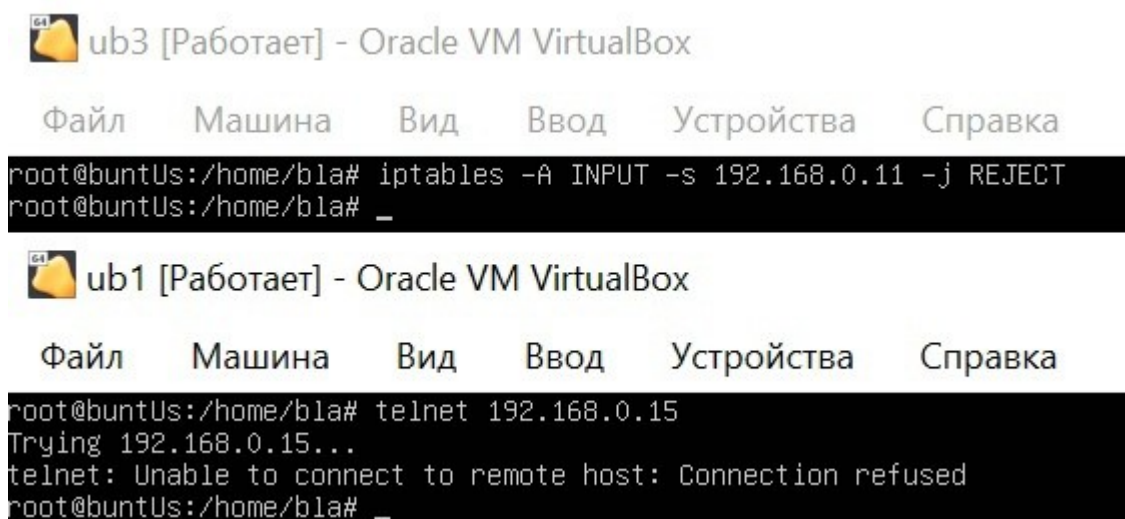
ub3 [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
root@buntUs:/home/bla# ifconfig -a
enp0s3   Link encap:Ethernet  HWaddr 08:00:27:4a:9d:7d
         inet addr:192.168.0.15  Bcast:192.168.0.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe4a:9d7d/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:80 errors:0 dropped:0 overruns:0 frame:0
         TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:17957 (17.9 KB)  TX bytes:4154 (4.1 KB)
```

Рисунок 0. Настройка виртуальных машин

1) Был заблокирован доступ с ub1 к ub3. Для проверки попробуем подключиться к ub3 с ub1

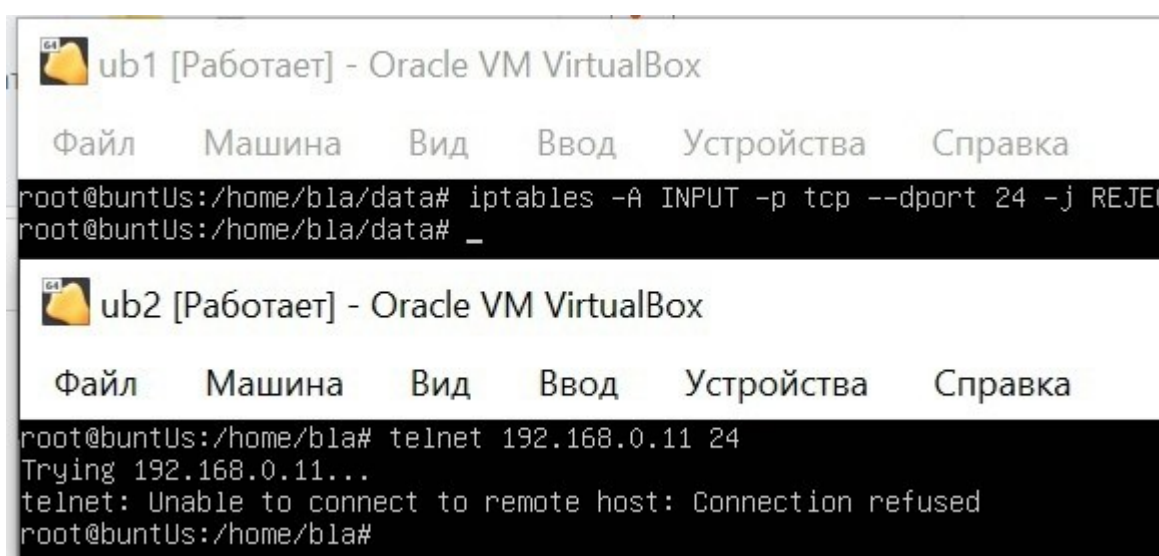


```
ub3 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla# iptables -A INPUT -s 192.168.0.11 -j REJECT
root@buntUs:/home/bla# _

ub1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla# telnet 192.168.0.15
Trying 192.168.0.15...
telnet: Unable to connect to remote host: Connection refused
root@buntUs:/home/bla# _
```

Рисунок 1. Подключение к ub3 с ub1 при фильтрации по IP-адресу

2) был заблокирован доступ по порту 24 на ub1, попробуем подключиться с ub2



```
ub1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla/data# iptables -A INPUT -p tcp --dport 24 -j REJECT
root@buntUs:/home/bla/data# _

ub2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla# telnet 192.168.0.11 24
Trying 192.168.0.11...
telnet: Unable to connect to remote host: Connection refused
root@buntUs:/home/bla#
```

Рисунок 2. Подключение к ub1 с ub2 при фильтрации по порту

3) был заблокирован доступ к порту 74 на ub3 от ub2. Как видно, с ub1 всё ещё можно подключиться, а с ub2 нет

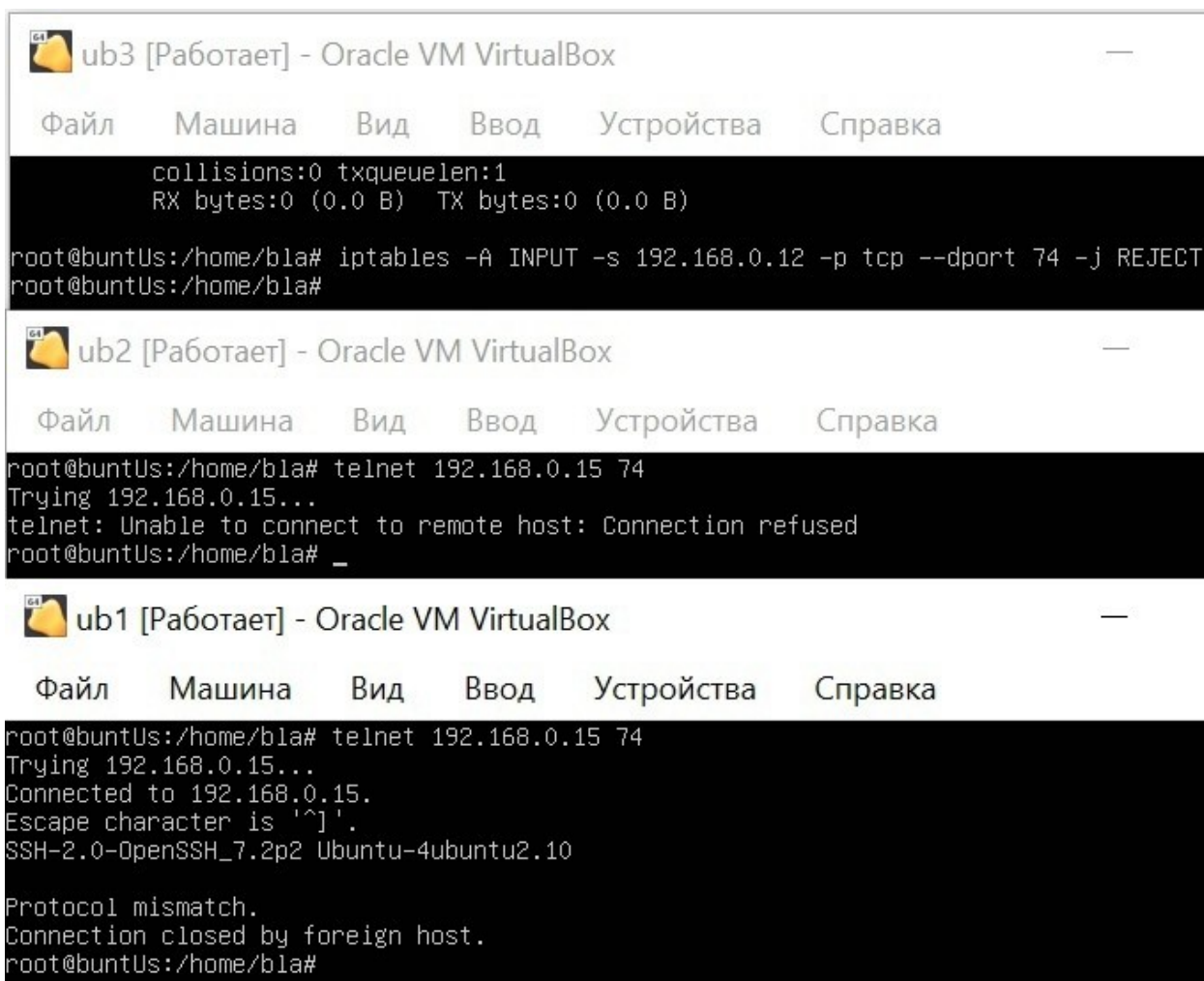
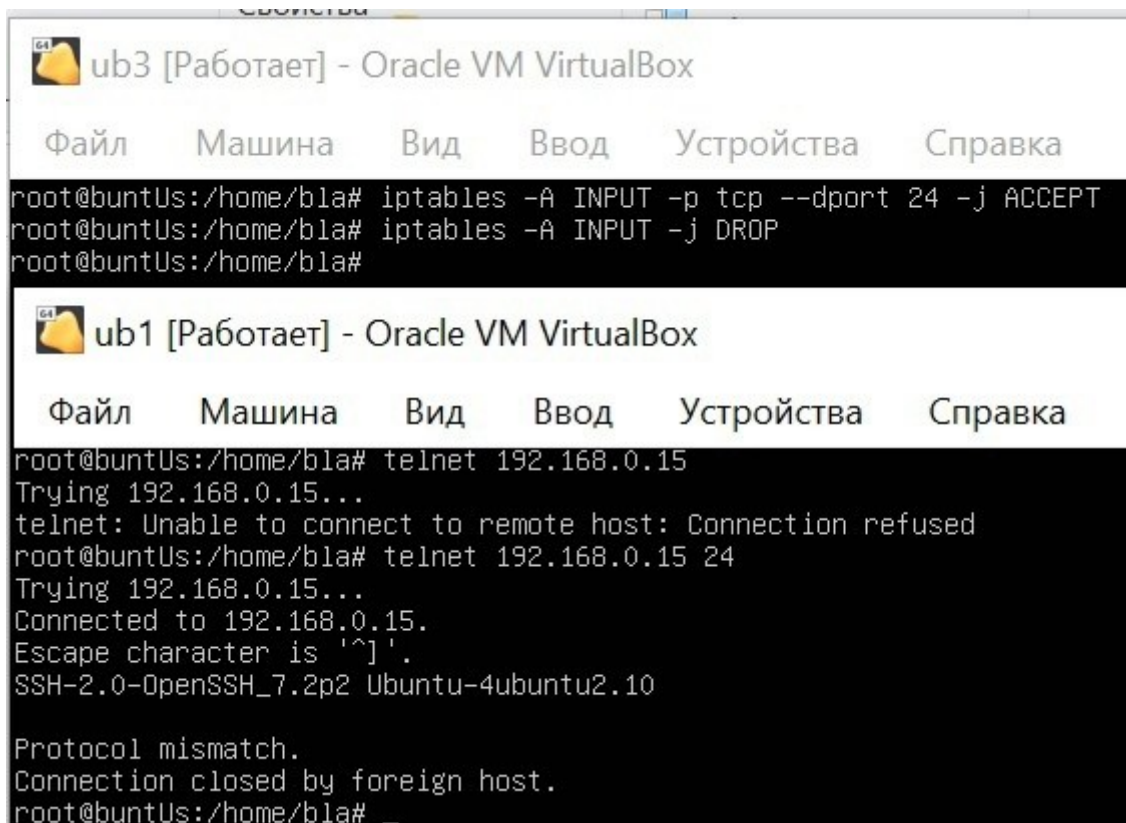


Рисунок 3. Подключение к ub3 с ub1 и ub2 при блокировке по порту

4) был запрещён доступ к ub3, можно было подключиться только по порту 24. Проверим, что по нему можно подключиться и сделаем это с ub1



```
ub3 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla# iptables -A INPUT -p tcp --dport 24 -j ACCEPT
root@buntUs:/home/bla# iptables -A INPUT -j DROP
root@buntUs:/home/bla#

ub1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla# telnet 192.168.0.15
Trying 192.168.0.15...
telnet: Unable to connect to remote host: Connection refused
root@buntUs:/home/bla# telnet 192.168.0.15 24
Trying 192.168.0.15...
Connected to 192.168.0.15.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10

Protocol mismatch.
Connection closed by foreign host.
root@buntUs:/home/bla# _
```

Рисунок 4. Подключение к ub3 по порту 24

5) была обеспечена блокировку всех входящих и исходящих пакетов узла Ub3, исключая пакеты управления сетью(протокол ICMP).

Были применены команды:

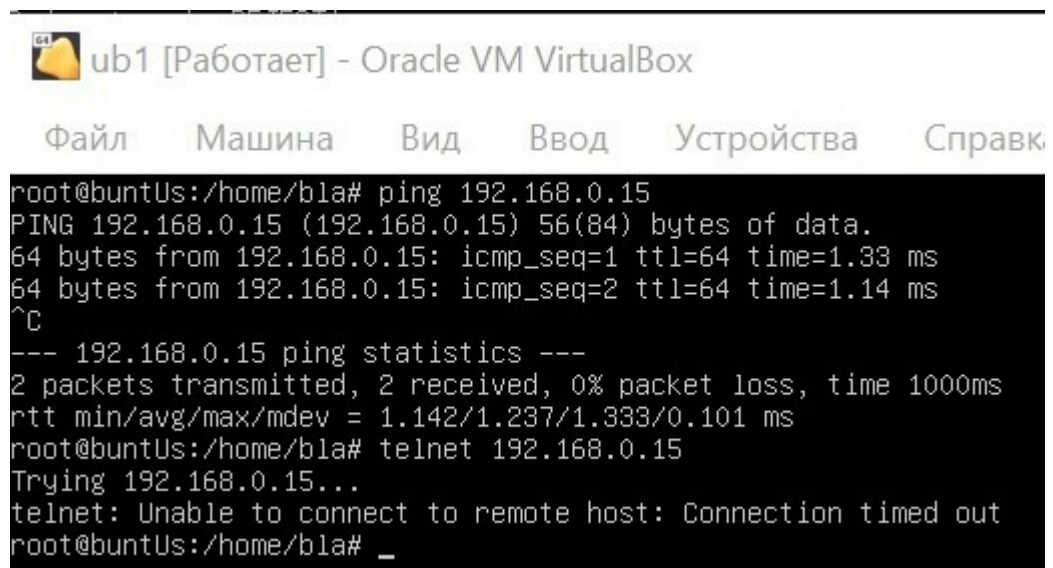
```
iptables -A INPUT -p icmp -j ACCEPT
```

```
iptables -A OUTPUT -p icmp -j ACCEPT
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

Было проверено, что Ub3 принимает и отвечает на запросы ко манды ping, но не отвечает на запросы протокола TCP



```
ub1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@buntUs:/home/bla# ping 192.168.0.15
PING 192.168.0.15 (192.168.0.15) 56(84) bytes of data.
64 bytes from 192.168.0.15: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from 192.168.0.15: icmp_seq=2 ttl=64 time=1.14 ms
^C
--- 192.168.0.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.142/1.237/1.333/0.101 ms
root@buntUs:/home/bla# telnet 192.168.0.15
Trying 192.168.0.15...
telnet: Unable to connect to remote host: Connection timed out
root@buntUs:/home/bla# _
```

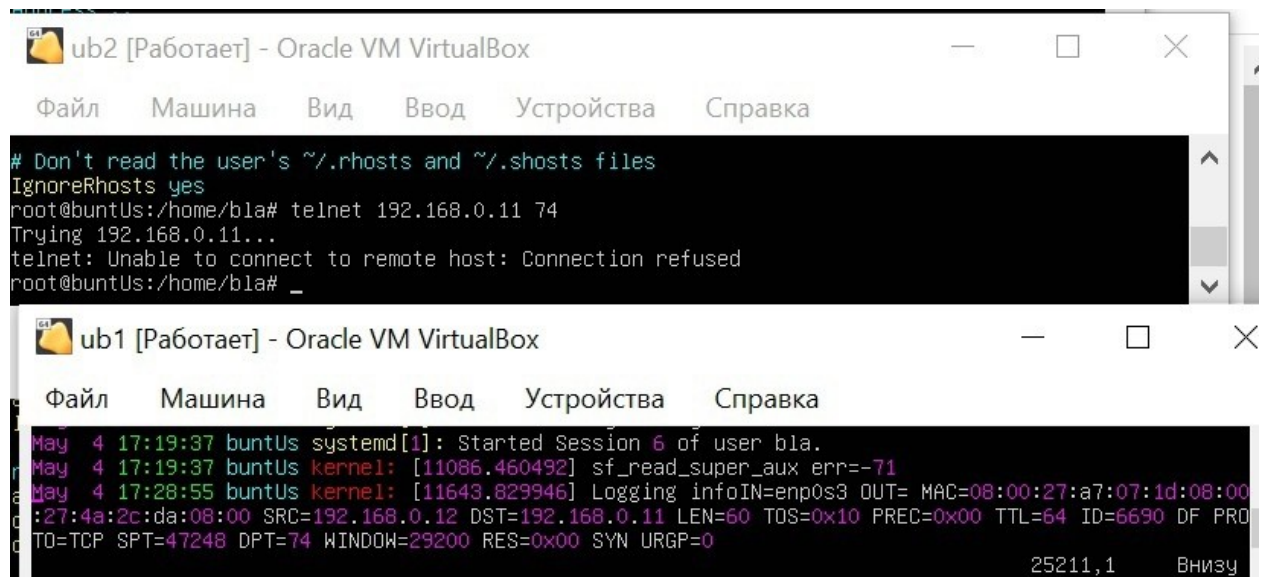
Рисунок 5. Подключение к ub3 по tcp и icmp

б) было запрещено подключение к Ub1 по порту 74. Было настроено логгирование попыток подключения по порту 74

Команды:

```
iptables -A INPUT -p tcp --dport 74 -j LOG --log-prefix "Logging info"
```

```
iptables -A INPUT -p tcp --dport 74 -j REJECT
```



```
ub2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
root@buntUs:/home/bla# telnet 192.168.0.11 74
Trying 192.168.0.11...
telnet: Unable to connect to remote host: Connection refused
root@buntUs:/home/bla# _

ub1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
May  4 17:19:37 buntUs systemd[1]: Started Session 6 of user bla.
May  4 17:19:37 buntUs kernel: [11086.460492] sf_read_super_aux err=-71
May  4 17:28:55 buntUs kernel: [11643.829946] Logging infoIN=enp0s3 OUT= MAC=08:00:27:a7:07:1d:08:00
:27:4a:2c:da:08:00 SRC=192.168.0.12 DST=192.168.0.11 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=6690 DF PRO
TO=TCP SPT=47248 DPT=74 WINDOW=29200 RES=0x00 SYN URG=0
25211,1  Внизу
```

Рисунок 6. Подключение к ub1 по порту 74 с логгированием

7) был заблокирован доступ по порту 14 к Ub3 с Ub1 по его MAC-адресу

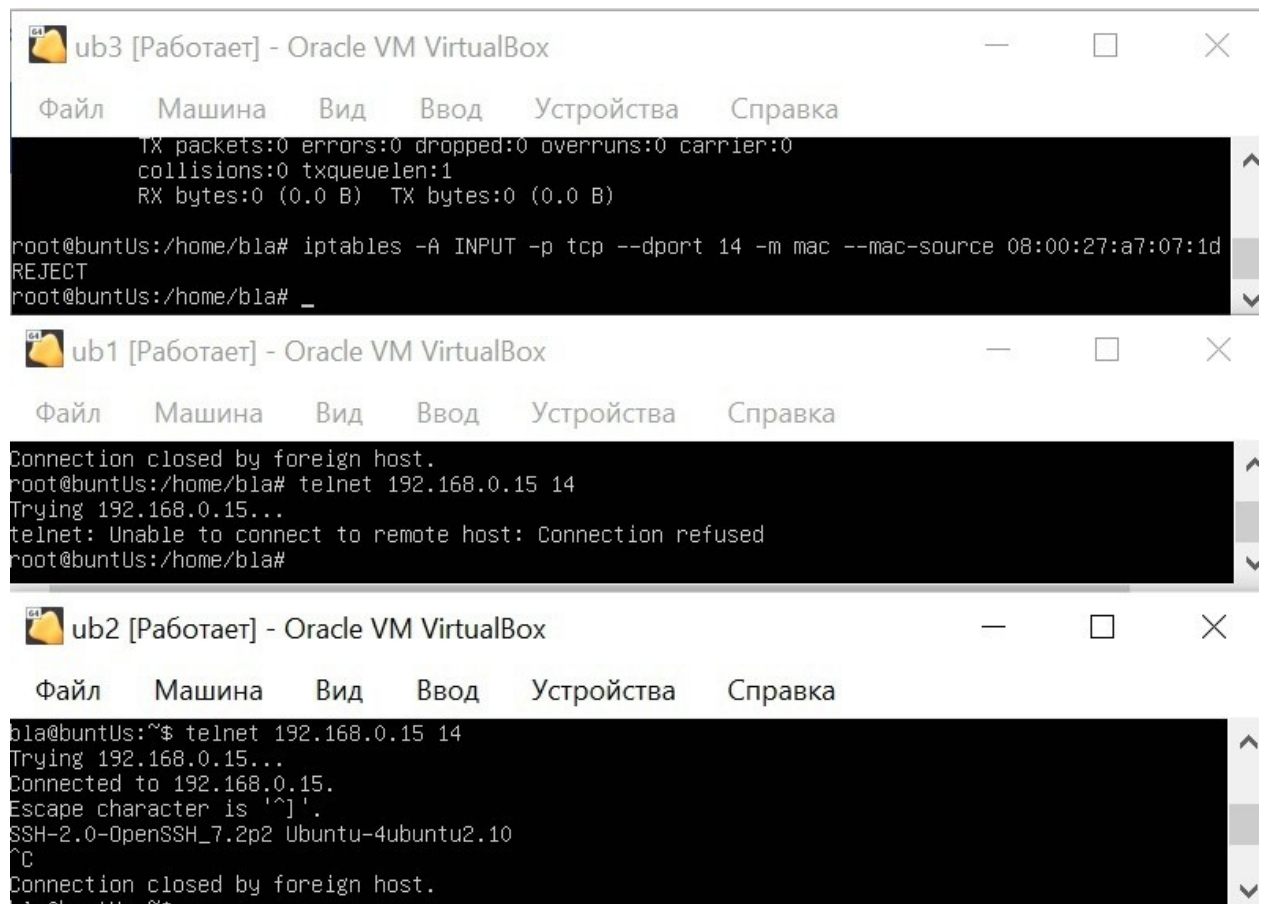


Рисунок 7. Проверка фильтрации на ub3 по mac-адресу

8) был полностью закрыт доступ к Ub1. Был разрешен доступ для Ub3 к Ub1, используя диапазон портов 14-74

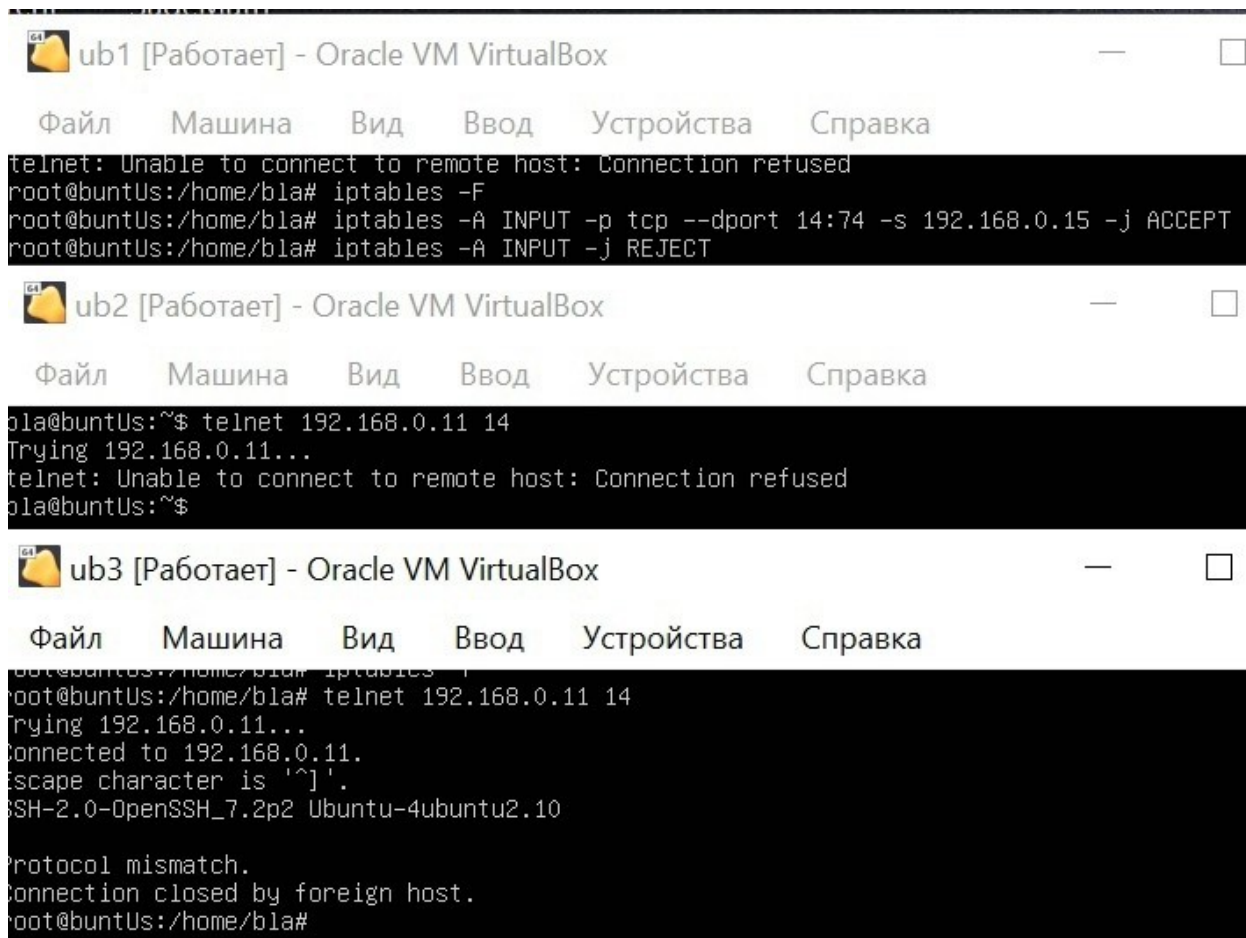


Рисунок 8-1. Подключение к ub1 по порту 14 из диапазона

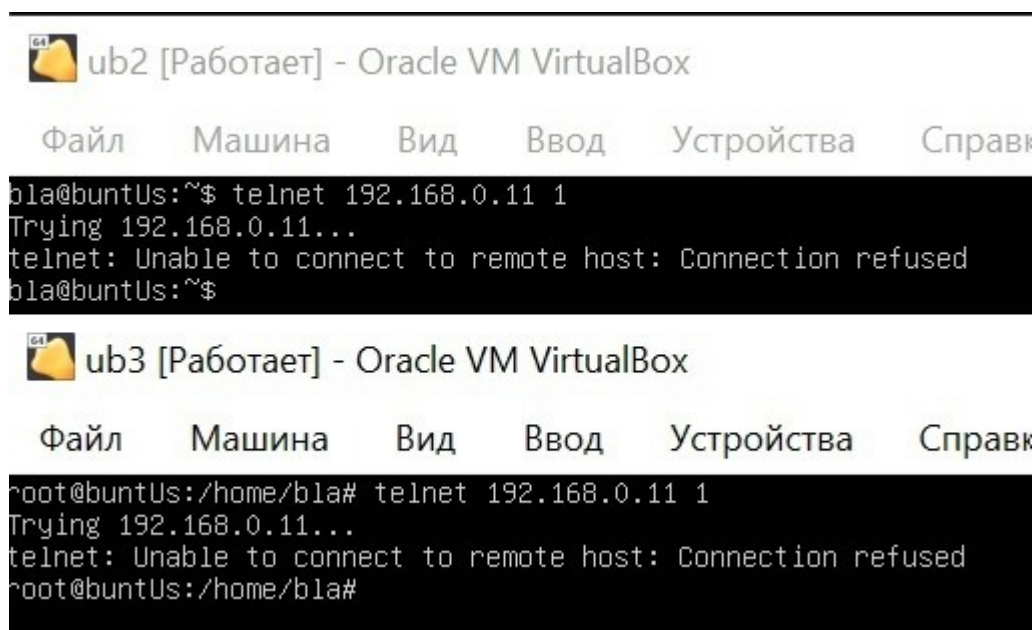


Рисунок 8-2. Подключение к ub1 по порту 1 — не из диапазона

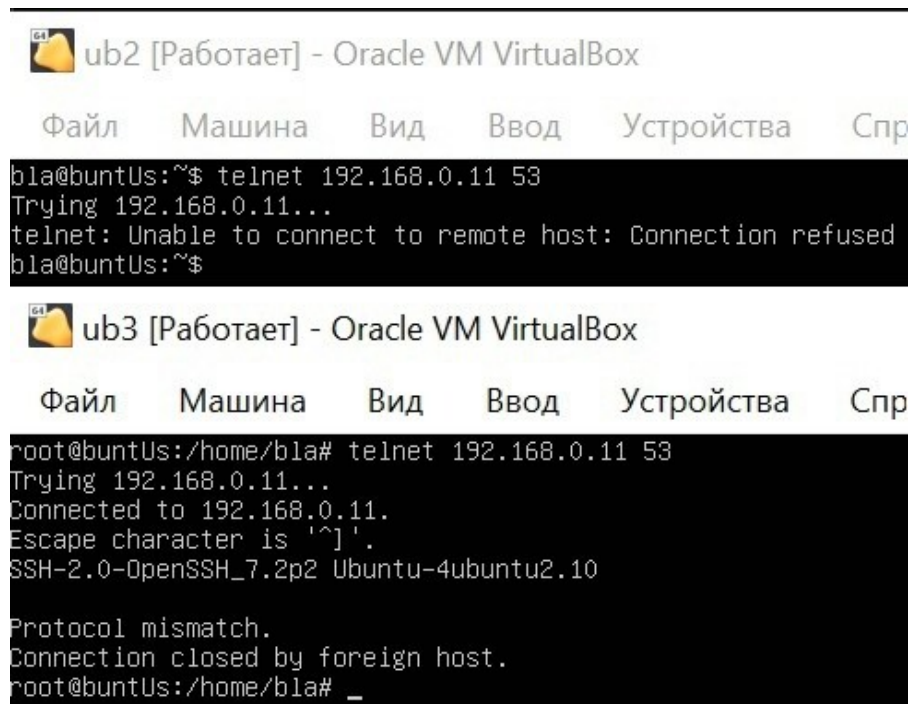


Рисунок 8-3. Подключение к ub1 по порту 53 из диапазона

9) было разрешено только одно ssh подключение к ub2

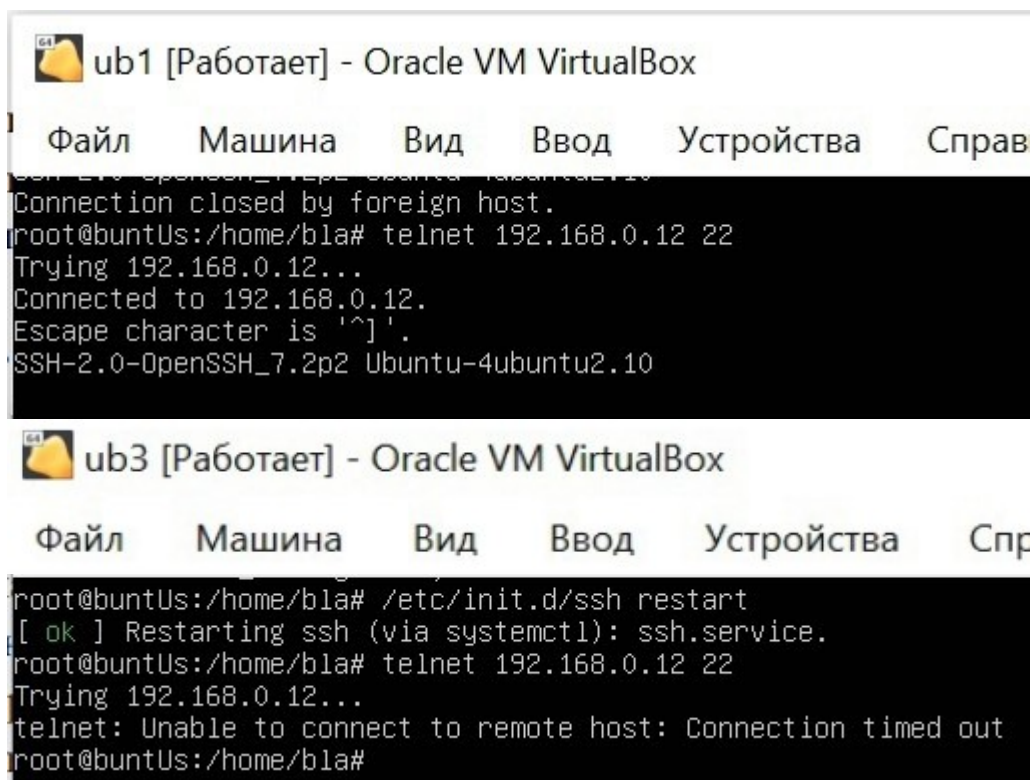


Рисунок 9. Проверка на возможность только одного ssh подключения к ub2

Ответы на контрольные вопросы.

1. Что позволяет делать сетевой экран?

Ответ: позволяет настраивать фильтрацию для сетевого трафика

2. Какие бывают типа сетевых экранов и чем они отличаются?

Ответ: есть два типа. Первый анализирует только заголовки пакетов и может работать на транспортном, сетевом и канальном уровнях иерархии DoD (TCP/IP). В данном варианте анализ входящих и исходящих пакетов осуществляется на основе информации, содержащейся в следующих полях TCP- и IP-заголовков пакетов: IP-адрес отправителя; IP-адрес получателя; порт отправителя; порт получателя. В зависимости от отслеживания активных соединений подобные сетевые экраны делятся на два типа: stateless (простая фильтрация) и stateful (фильтрация с учетом контекста).

Второй тип межсетевого экрана может анализировать данные в пакете и работает на прикладном уровне иерархии DoD (TCP/IP). Благодаря работе на прикладном уровне можно организовать большое число проверок, которые будут использовать особенности работы протоколов прикладного уровня. Например, можно добавить проверку взлома известных «дыр» в программном обеспечении и протоколах.

3. Приведите примеры, когда лучше использовать host-based сетевые экраны.

Ответ: когда сеть небольшая или правил фильтрации немного

4. Каким типом сетевого экрана является iptables?

Ответ: host-based, а также stateles

5. Какие есть минусы использования в качестве сетевого экрана проху-сервера?

Ответ: трафик проходит через сторонний узел, на нём он может был использован во вредоносных целях(если это арендованный прокси), также может быть ситуация «бутылочного горлышка»

6. Для чего нужна таблица nat в iptables?

Ответ: чтобы иметь доступ ко внешним сетям (для настройки NAT и MASQUERADE, например)

7. Чем DROP отличается от REJECT?

Ответ: REJECT отбрасывает пакет и отправляет ответ, что соединение невозможно, а DROP крашит его молча

8. Чтобы заблокировать доступ с ПК на ресурс во внешней сети какую цепочку лучше использовать?

Ответ: OUTPUT

9. Можно ли использовать несколько типов сетевых экранов для защиты корпоративных сетей и узлов и почему/для чего?

Ответ: можно, например, для фильтрации на различных уровнях. Допустим, чтобы из интернета не приходили пакеты с конкретных IP-адресов, а внутри сети между узлами фильтрация происходила с учётом контекста

Выводы.

Были изучены принципы работы с сетевыми экранами. Были получены навыки фильтрации пакетов по их принадлежности к определённым IP-адресам, мас-адресам, портам.